Approach to Developing a Maritime Cybersecurity Virtual Training Environment

Borislav Nikolov
Department of Information Technologies
Nikola Vaptsarov Naval Academy
Varna, Bulgaria
nikolov@naval-acad.bg

***Abstract.* The maritime industry is increasingly reliant on digital systems for navigation, communication, cargo management, and other critical functions. As these systems become more interconnected and technologically advanced, they also become vulnerable to cyber threats. A virtual training environment allows maritime personnel to simulate cyber attacks and practice responding to them, enhancing their preparedness and resilience against real-world cyber threats. Cyber attacks targeting maritime assets can have severe consequences, including disruptions to operations, financial losses, environmental damage, and even threats to human safety. By providing virtual training environments, maritime organizations can identify and mitigate cybersecurity risks before they escalate into actual incidents, thereby safeguarding their assets and operations.**

Regulatory bodies, such as the International Maritime Organization (IMO) and various national maritime authorities, have established guidelines and regulations aimed at enhancing cybersecurity in the maritime sector. Developing a virtual training environment enables maritime organizations to ensure compliance with these regulations by training personnel on cybersecurity best practices and regulatory requirements. Conducting hands-on cybersecurity training in a real-world maritime environment can be logistically challenging and costly. A virtual training environment offers a cost-effective alternative by allowing personnel to engage in realistic cybersecurity scenarios without the need for physical equipment or resources.

This paper presents an approach to developing a maritime cybersecurity virtual training environment utilizing open-source software.

Keywords: cybersecurity, virtual training environment, cyber hygiene, training scenarios, computer virtualization.

I. Introduction

The maritime industry is changing rapidly and becoming increasingly digital. Ships, ports, and related infrastructure are increasingly using digital systems to manage crews, cargo, communications, and more [1]. As connectivity and automation grow, so does the potential for cyberattacks. The maritime industry is exposed to a variety of cyber threats, including hacker attacks, phishing, malware, and more. These threats can pose a risk to the safety of crews, the protection of personal data, the integrity of management systems, and other aspects of maritime transport [2].

International regulations, such as the ISPS Code [3] and the ISM Code [4], impose strict security requirements on the maritime industry. In recent years, new legislative frameworks have emerged specifically dedicated to cyber security in this industry.

Cyber attacks can cause serious damage to the maritime business, from financial losses and data breaches to serious damage to a company's reputation [2]. Cybersecurity training helps crew to understand potential threats and take appropriate protection measures. Training not only provides technical knowledge and skills but also builds a cyber security culture within the company. This means that all employees, from ship crews to port managers, understand the importance of cyber security and are committed to achieving and maintaining security [5].

Cybersecurity training conducted in a virtual training environment (VTE) offers numerous advantages that make it a preferred choice for many organizations and industry participants [6]. The VTE enables the creation of realistic simulations of cyber attacks, threats, and scenarios that can be used for training. Such simulations allow learners to become familiar with different types of threats and develop skills to recognize and deal with them. The VTE provides a secure and controlled platform for conducting cybersecurity training. This allows learners to experience various cyber attack scenarios without the real risks associated with malicious activities on real systems. Virtual cybersecurity training is flexible and accessible to trainees from different locations and at any time. This allows employees, especially those in the maritime industry, to receive training without needing to be physically present in specially equipped training labs or centers [7].

Print ISSN 1691-5402
Online ISSN 2256-070X
https://doi.org/10.17770/etr2024vol2.8039

Learning in a virtual environment very often offers interactive learning materials including exercises, tests, simulations, and games. These learning elements can improve learner engagement and interest, accelerating their acquisition of new knowledge and skills.

Delivering cybersecurity training in a virtual environment is often more cost-effective than traditional face-to-face courses. This reduces the costs of travel, and rental of premises and equipment, which are usually associated with the organization of training [8].

Conducting cybersecurity training in a virtual environment requires a specialized simulation environment to provide the various training scenarios. Acquiring simulation environments such as Cyber Range is a costly investment for any maritime company or training institution [6]. However, there are also technical solutions based on open-source programs that can have the same efficiency, but at a significantly lower cost. In any case, it should be kept in mind that the instructors and the training materials and scenarios developed by them remain the key elements in conducting cybersecurity training [9], [10].

II. DEFINING CYBERSECURITY VIRTUAL TRAINING ENVIRONMENT

How a virtual training environment will be used depends primarily on the target categories of participating trainees. These categories define the requirements for the methods to access the virtual environment and what real devices are to be simulated [11].

If the training will be related to cybersecurity, the target groups of trainees are mainly two categories. The first category is related to the users with administrative access to IT systems and has responsibilities for ensuring the general level of cyber security. The second category of users can be broadly described as end-users of IT systems. When the training is focused on cybersecurity in the maritime industry additional requirements arise – the VTE must provide the possibility of remote secure access as well as simulate the ship systems that are quite specific.

Both categories of trainees should be able to remotely and locally access different simulation scenarios based on their daily activities as part of the ship's crew or employees in the IT support department in the companies' shore offices [12].

Fig. 1 presents the different access methods for both trainees' categories – “Advanced User” and “Beginner User”. The “Advanced User” represents the users with administrative access to IT systems, and the “Beginner User” represents the end-users of IT systems. It should be noted that the differences between cybersecurity training in the maritime industry and any other industry will be in the type of simulated devices and scenarios from the VTE.

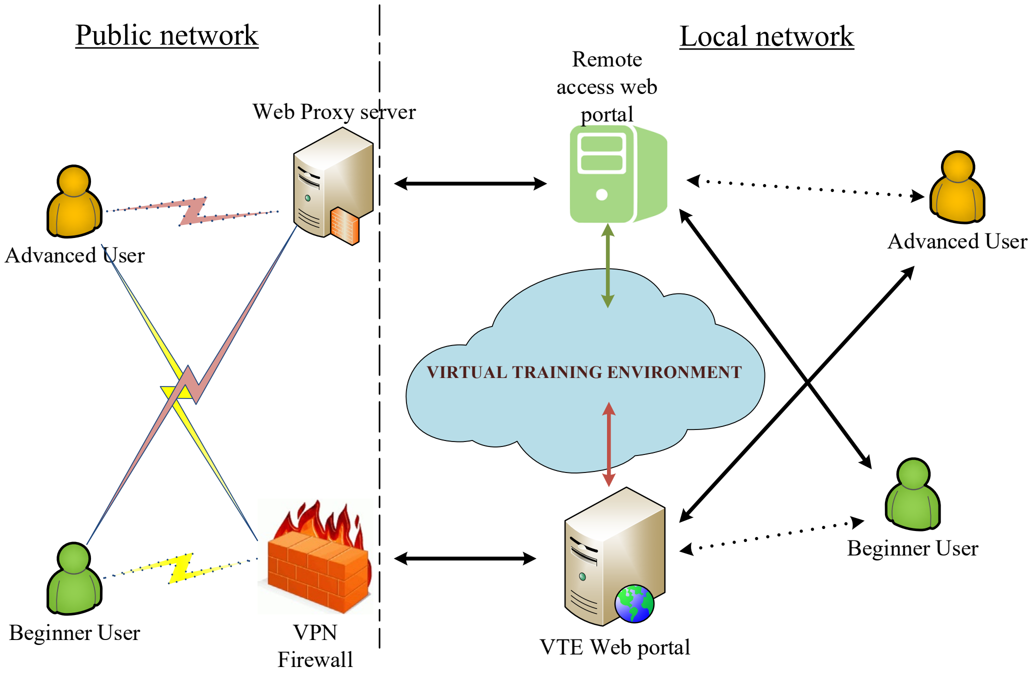

Fig. 1. Remote and local access to the maritime cybersecurity virtual training environment.

The VTE resource access topology presented in Fig. 1 has two main zones – “Public network” and “Local network”. “Public network” represents the ability for remote access to the VTE from anywhere by using an Internet connection. At the same time, the “Local network” represents the ability for local access to the VTE at the training centers where the VTE is installed.

The VTE used for cybersecurity training is most often called “Cyber Range” [13]. This environment consists of multiple virtual machines that represent computers, servers, network equipment, and other IT devices with their configurations and vulnerabilities. The main access method to the virtual machines is through the internal VTE web portal. However, direct access to virtual machines is possible if they are configured with RDP, SSH, Telnet, VNC, or other remote access protocols. In this case, the access can be simplified using a remote desktop gateway like Apache Guacamole or a similar platform [14].

The two defined trainees' categories require different access types to the virtual devices. The Beginners need access to a single simulated end-user desktop. This access can be provided by direct access to the VTE web portal.

This scenario is useful only if the trainee is located at the training center, but more useful will be the access through a remote desktop gateway. If the trainee is out of the training center, access should be provided through a remote desktop gateway. That will provide more security. A VPN Firewall or other VPN concentrator can be used if the highest level of security is required for remote access.

Contrariwise, the Advanced trainees will require access to multiple devices at the same time depending on the training scenario. Again, the access can be provided by direct access to the VTE web portal, but only if the trainee is located at the training center. Because access to multiple virtual devices will be required for this type of trainee, the remote access web portal is not recommended due to the peculiarities of simultaneous operation with multiple remote terminals. Remote Advanced trainees will need a VPN connection to perform all tasks in the training scenario.

In any case, access to the remote desktop gateway outside the training center must be provided only through a web proxy server. This will ensure a relatively good level of access security.

In Fig. 1 the main access methods are presented with solid lines. The dotted lines present access methods that should be used as a last resort.

Fig. 2 presents the VTE main functions and modules that are required to support cybersecurity training.

VTE utilizes computer virtualization technology to simulate server and desktop operating systems as well as network or other communication equipment. At least one physical host is the root of the VTE. Different hypervisors or server OS that support containerization can be installed on the physical host.

The VTE software should provide several mandatory functions as follows:

- Virtual Nodes Management;
- Labs Management;
- Account Management;
- User-friendly Web interface.

The Virtual Nodes Management function provides capacity for the simulation of a wide range of server and desktop operating systems, hypervisors, physical hosts (computers or servers), storage systems, network and communication devices and equipment. This function can be determined as one of the two core functions of any VTE. It is required for VTE to have the capacity to simulate as much as possible different types of nodes.

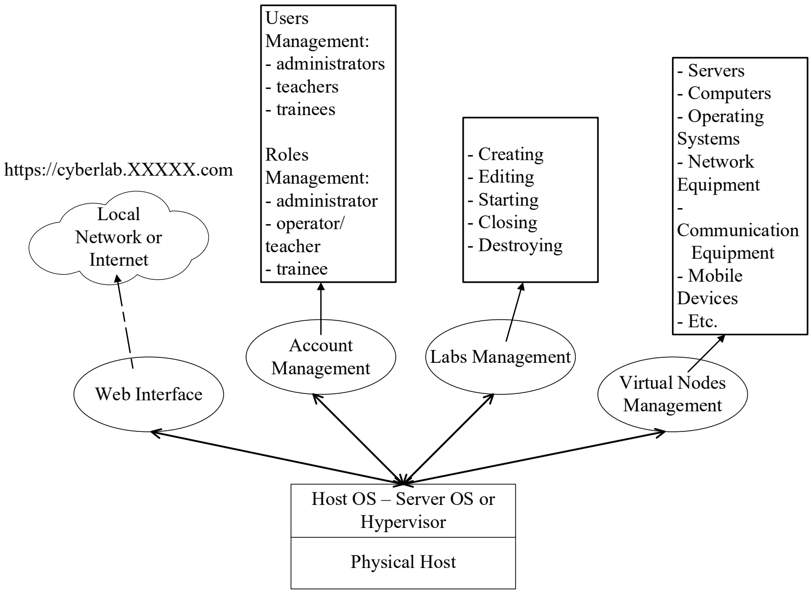

Fig. 2. Cybersecurity VTE main functions and modules.

The Labs Management function is the second core function of any VTE. Utilizing this function VTE administrators (or operators) can develop virtual labs combining virtual nodes. These labs are used in different scenarios during cybersecurity training. Labs are assigned to the trainees. Labs Management must have the ability to restore labs to their initial state after every training.

The Account Management function is required to define VTE users' roles. At least three users' roles should be preset – administrator, operator or teacher, and trainee or student.

Administrators are responsible for the whole VTE system:

- Normal operation of the system and its accessibility from users;
- Managing virtual nodes;
- Managing users and users' roles.

Operators or teachers are responsible for developing the virtual labs and their assignment to the trainees or students.

Trainees or students are the end users of the VTE. Trainees or students use the VTE according to their curriculum or training scenarios. Different trainees' categories were described above.

As already noted, the users access the VTE resources over a computer network, and most often the access is through the VTE web interface or remote access web gateway. VTE web interface should provide easy access without compromising security.

III. MARITIME CYBERSECURITY VTE AT NIKOLA VAPTSAROV NAVAL ACADEMY

Based on the functions presented in the previous section, Nikola Vaptsarov Naval Academy (NVNA) built a maritime cybersecurity VTE utilizing open-source software. This VTE uses a Moodle learning management system (LMS) to provide different cybersecurity training scenarios [15].

The physical host used to build the VTE has two Intel(R) Xeon(R) CPU E5-2620 processors and 72 GB RAM. The operating system installed on the host is Ubuntu 18.04.6 LTS. The industry-standard container runtime *containerd* version 1.6.12 is installed to support virtual devices used in labs. To ensure the cybersecurity of the IT infrastructure in which VTE is built, isolation of the VTE's VLANs from the NVNA's computer network has been implemented. Local and remote trainees can access only the virtual machines and data from the VTE. The isolation of the VLANs ensures that a simulated for training purposes cyberattack will not reach the productive environment. The network traffic over public networks uses secured protocols.

The VTE status information page (Fig. 3) presents information about the current load of the system. The built system has enough computing resources to support all running simultaneously labs that are required to provide cybersecurity training at NVNA.

For each training, at least one virtual lab providing the teacher's (instructor's) topology (Fig. 4) and one lab for each student (Fig. 5) are required. In NVNA, a policy was adopted for the practical maritime cybersecurity classes to be held in groups of between 4 and 8 trainees. This means that every training requires between 5 and 9 labs.

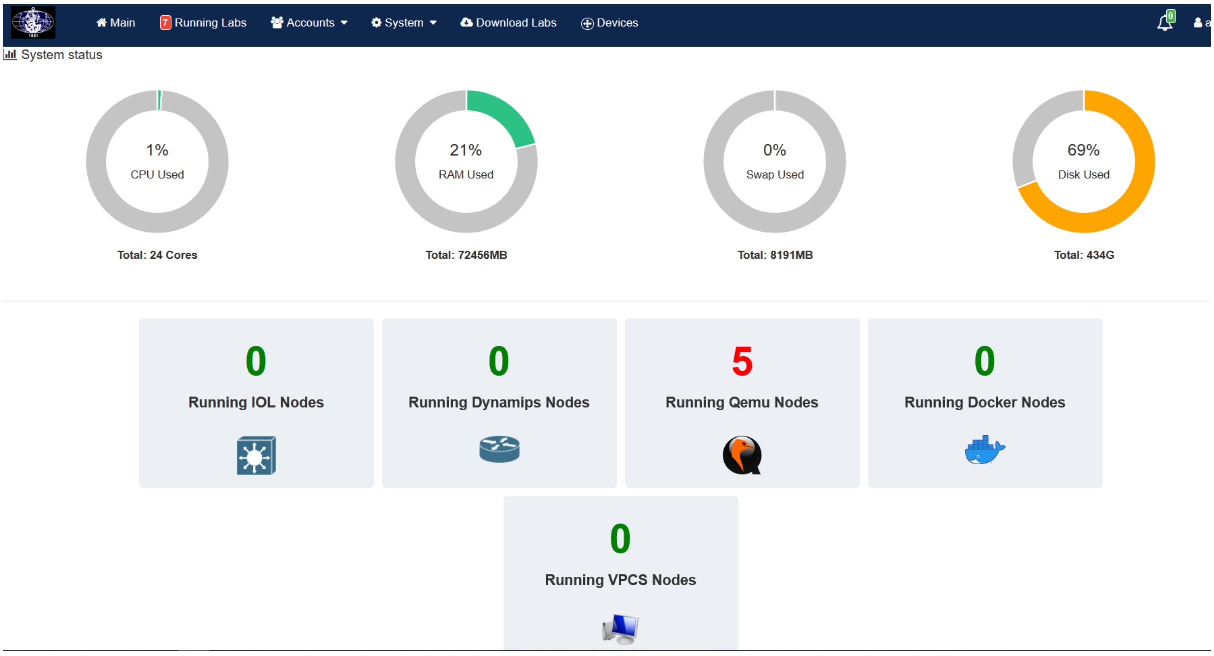

Fig. 3. NVNA cybersecurity VTE system status information page.

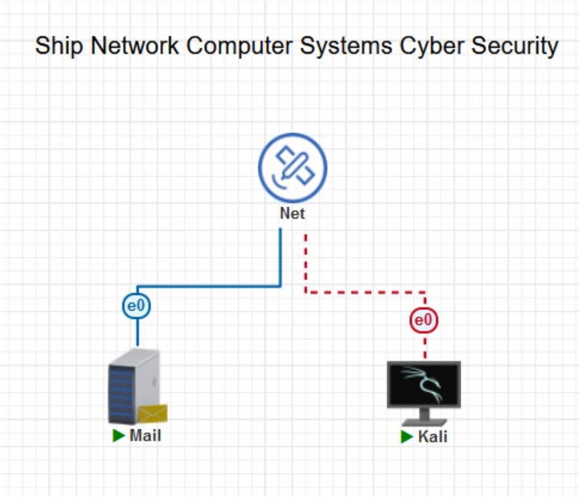

Fig. 4. NVNA cybersecurity VTE teacher's (operator's) virtual topology.

Virtual devices used in the teacher's and student's topologies are different and have different purposes. The teacher's topology has to include the virtual devices that will be used to provide the main part of the training scenario, whereas the student's topology has to include the virtual devices that will perform the role of the "target" machines in a simulated cyber attack.

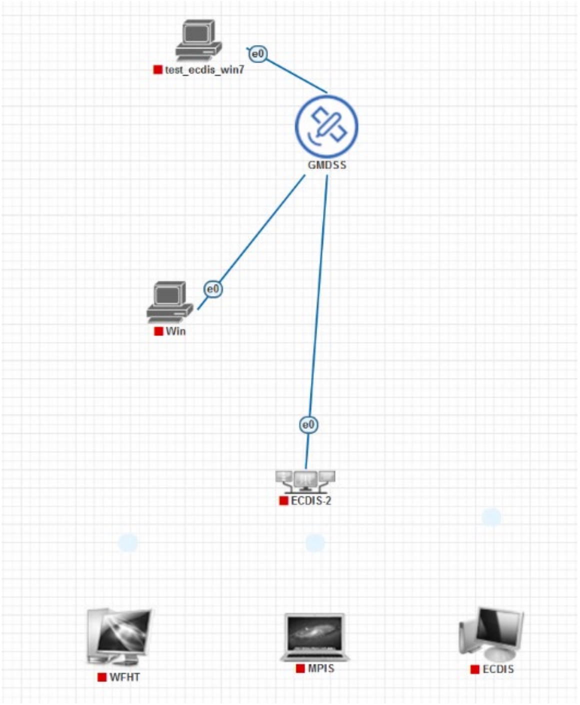

Fig. 5. NVNA cybersecurity VTE trainees' (students') virtual topology.

The NVNA's cybersecurity VTE can provide training under several scenarios as follows:

- End-user device's operating system misconfiguration;
- Sensitive data unauthorized access;
- Phishing emails;
- Malware hidden behind commonly used file extensions;
- Ransomware;
- Privilege escalation;
- Social engineering countermeasures.

The teacher's topology (Fig. 4) consists of three elements – two virtual machines ("Mail" and "Kali") and one virtual network ("Net"). "Net" presents the connectivity to the other devices in the VTE. The virtual machines "Mail" and "Kali" are used to start cyber attacks against the students' topologies (students' labs) based on the training scenario. Other elements can be added to this topology if it is required by the training scenario. It should be noted that one teacher's topology can be used in more than one training scenario.

The student's topology (Fig. 5) consists of more elements because, in one training scenario, it has to provide a simulation of multiple vulnerable devices and systems. On this topology, it seems that some of the virtual devices are not connected to the virtual network "GMDSS". This is only apparent – all virtual devices are connected to the network, but for scenario purposes, it doesn't matter how some of the devices are connected.

A remote access web portal based on Apache Guacamole and HAproxy systems (Fig. 6) is used in NVNA. The purpose of this web portal is to provide access to the VTE's virtual devices for remote trainees. The web portal provides remote desktop access to a single VTE device or multiple VTE devices with a single user login. This web portal in conjunction with the NVNA's Moodle LMS is a complete solution for remote cybersecurity trainees.

A pilot maritime cyber hygiene course was conducted in NVNA with local trainees. Work is underway to organize and conduct a pilot course with remote trainees.

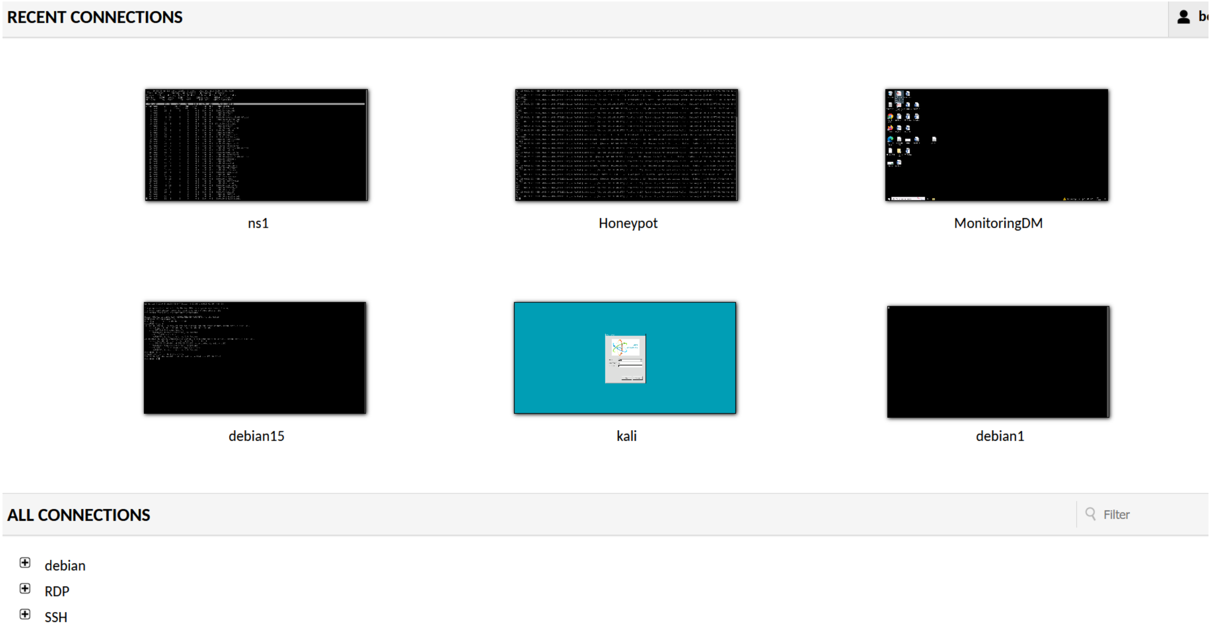

Fig. 6. NVNA's remote access web portal.

IV. Conclusions

Several open-source platforms have been integrated into NVNA to develop a maritime cybersecurity virtual training environment. This integrated solution has the same functionalities as a full-scale Cyber Range system. The future improvement of the system built in this way should be related to the tools for the automation of training scenarios development. This will enable trainees to perform the training scenarios without the involvement of teachers (instructors).

Acknowledgments

This work was supported by the National Scientific Program “Security and Defense”, adopted with RMS No. 731/21.10.2021, and financed by the Ministry of Education and Science of the Republic of Bulgaria according to Agreement No. D01-74/19.05.2022.

References

[1] P-L Sanchez-Gonzalez, D. Díaz-Gutiérrez, T.J. Leo, and L.R. Núñez-Rivas, “Toward Digitalization of Maritime Transport?”, Sensors, Vol. 19, Iss. 4, 2019. https://doi.org/10.3390/s19040926

[2] C-H Chang, S. Wenming, Z. Wei, P. Changki, and Ch. Kontovas, Evaluating cybersecurity risks in the maritime industry: a literature review. In: Proceedings of the International Association of Maritime Universities (IAMU) Conference, October 29 – November 01, 2019, Tokyo, Japan.

[3] International Maritime Organization, The International Ship and Port Facility (ISPS) Code, July 1, 2004.

[4] International Maritime Organization, International Safety Management Code, July 1, 1998.

[5] M. Canepa, F. Ballini, D. Dalaklis, and S. Vakili, Assessing the effectiveness of cybersecurity training and raising awareness within the maritime domain, 15th International Technology, Education and Development Conference, March 8-9, 2021, INTED2021 Proceedings, pp. 3489-3499. https://doi.org/10.21125/inted.2021.0726

[6] G. Potamos, A. Peratikou, and S. Stavrou, Towards a Maritime Cyber Range training environment, IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 2021, pp. 180-185. https://doi.org/10.1109/CSR51186.2021.9527904

[7] C. Willems and C. Meinel, Online assessment for hands-on cyber security training in a virtual lab, Proceedings of the 2012 IEEE Global Engineering Education Conference (EDUCON), Marrakech, Morocco, 2012, pp. 1-10. https://doi.org/10.1109/EDUCON.2012.6201149

[8] C. J. Bonk, Online training in an online world. Bloomington, IN: CourseShare.com, 2002.

[9] Ge Jin, Manghui Tu, Tae-Hoon Kim, J. Heffron, and J. White, Game based Cybersecurity Training for High School Students, SIGCSE '18: Proceedings of the 49th ACM Technical Symposium on Computer Science Education, February 2018, pp. 68-73. https://doi.org/10.1145/3159450.3159591

[10] T. van Steen and J. R.A. Deeleman, “Successful Gamification of Cybersecurity Training”, Cyberpsychology, Behavior, and Social Networking, 24:9, pp. 593-598, 2021. https://doi.org/10.1089/cyber.2020.0526

[11] V. Krinickij and L. Bukauskas, “Challenges in Cybersecurity Group Interoperability Training”, In: Stephanidis, C., Antona, M., Ntoa, S., Salvendy, G. (eds) HCI International 2023 Posters. HCII 2023. Communications in Computer and Information Science, vol 1834. Springer, Cham. 2023. https://doi.org/10.1007/978-3-031-35998-9_38

[12] M. Domínguez, D. Pérez, A. Morán, S. Alonso, M. A. Prada, and J. J. Fuertes, Remote training in cybersecurity for industrial control systems, 13th IFAC Symposium on Advances in Control Education ACE 2022: July 24 – 27, 2022, Hamburg, Germany. Vol. 55, Iss. 17, pp. 320-325, 2022. https://doi.org/10.1016/j.ifacol.2022.09.299

[13] M. M. Yamin, B. Katt, and V. Gkioulos, “Cyber ranges and security testbeds: Scenarios, functions, tools and architecture”, Computers & Security, Vol. 88, 2020. https://doi.org/10.1016/j.cose.2019.101636

[14] I. Hassan, “Levereging Apache Guacamole, Linux LXD and Docker Containers to Deliver a Secure Online Lab for a Large Cybersecurity Course”, 2022 IEEE Frontiers in Education Conference (FIE), Uppsala, Sweden, 2022, pp. 1-9. https://doi.org/10.1109/FIE56618.2022.9962510

[15] B. Nikolov and Y. Tsonev, Utilizing Moodle and Apache Open Meetings in a Learning Management System. In: SECOND CONFERENCE ON INNOVATIVE TEACHING METHODS (ITM 2017) June 28-29, 2017, Varna, Bulgaria.

[16] I. Chakarov, “Cyber Security as Part of the Contemporary Security Environment”, NRDC-GR Herald Magazine, Iss. № 8, pp. 7-10, July 2016 – January 2017.